Smarter SCADA for Oil and Gas – Workshop
October 2, 2012
## Agenda – Smarter SCADA Workshop (9am – 4:00pm)

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
</tr>
</thead>
<tbody>
<tr>
<td>9:00am</td>
<td>BREAK</td>
</tr>
<tr>
<td>9:15am</td>
<td>Components of Smarter SCADA</td>
</tr>
<tr>
<td>9:30am</td>
<td>Smarter SCADA Connectivity</td>
</tr>
<tr>
<td>10:15am</td>
<td>BREAK</td>
</tr>
<tr>
<td>10:30am</td>
<td>Hands on Connectivity Workshop</td>
</tr>
<tr>
<td>12:30am</td>
<td>LUNCH</td>
</tr>
<tr>
<td>1:30pm</td>
<td>SCADA Device Security</td>
</tr>
<tr>
<td>2:00pm</td>
<td>Operational Control &amp; Decision Management</td>
</tr>
<tr>
<td>2:30pm</td>
<td>BREAK</td>
</tr>
<tr>
<td>2:45pm</td>
<td>Applying Smarter SCADA to your Scenarios</td>
</tr>
<tr>
<td></td>
<td>Next Steps</td>
</tr>
</tbody>
</table>

Smarter Oil and Gas

- Instrumented
- Interconnected
- Intelligent
Components of Smarter SCADA
October 2, 2012
Agenda

- Quick Review
  - What Problems are we Addressing?

- Smarter SCADA Architecture

- Technology Components
  - Core
  - Additional
What are oil and gas companies wanting to address?

- Mitigation of environmental risk
- Earlier detection of leaks
- Faster problem resolution
- More effective management of audit and regulation
- More efficient operations.

What’s getting in the way?

Effort / Cost / Time:

- To pull information from SCADA systems
- To deliver information to all the places where it is needed
- To correlate events and identify patterns and problems BEFORE they happen
- To ensure secure access to / from devices.
Current State of SCADA…

Positive Aspects
- Fit for Purpose
- Real-time
- Stateful

Negative Aspects
- Poll/Response Consumes 100% of Bandwidth
- Round Robin Polling Produces High Latency on Alarms/Alerts
- The Protocol “is” the Transport
- One-to-One Data Relationship
- Legacy Protocol & Equipment “Catch 22”
- No Authentication or Security
- Hardcoded Connections to Each Enterprise App
- Riddled with points of intrusion
Smarter SCADA – Ultimate Architecture

- Connect all hosts (SCADA and Telematics) into the same infrastructure
- Implement mobile dashboards for field technicians
- Implement a Centralized Data Warehouse / Historian
- Implement a Centralized Event Correlator
- Implement an Enterprise Asset Management system
Smarter SCADA – How do we get there?

Initial Steps:
- Decouple the devices from the SCADA host
- Replace communications between devices and the SCADA host with MQTT (open device protocol)
- Insert Message Broker as communications hub

Value of MQTT:
- Lowers bandwidth consumption
- Decouples data from transport
  - Enables one-to-many data relationship
  - Enables authentication and access control
  - Enables quality of service (e.g., assured delivery)
  - Sends notification if device goes offline.
Components of Smarter SCADA

- **Core Components**
  - IBM WebSphere MQ / MQTT
  - IBM WebSphere Message Broker

- **Additional Components**
  - Mobile SCADA Dashboards
  - Centralized Data Warehouse / Historian
  - Centralized Event Correlation
  - Enterprise Asset Management
IBM WebSphere MQ: The Universal Message Bus

- A single enterprise messaging solution for delivery of any kind of data anywhere. MQ moves:
  - Data
  - Messages
  - Files
  - Events
  - Services

- Provides a comprehensive range of messaging capabilities to support business requirements:
  - Qualities of Service (QoS)
  - Reliability and high availability
  - Messaging integration patterns
  - Managed file transfer
  - End-to-end security

- Provides data access and privacy controls to meet audit and regulatory requirements.
WebSphere MQ Security – Unified Enterprise Intrusion Protection

WebSphere MQ

- A proven security solution used in banking, insurance, military, …
- Single unified approach to security
  - Encryption
  - Authorization
  - Authentication
- Single Policy Enforcement Point (PEP)
  - Reduces the number of points of vulnerability
  - Reduces complexity
  - Provides the capability to address exposures faster.

SCADA networks are only as strong as their weakest link.
MQTT – a component of IBM WebSphere MQ

- MQTT = MQ Telemetry Transport
- In a nutshell
  - “An open lightweight event and message oriented protocol allowing devices to communicate efficiently across constrained networks to backend systems”
- Aimed at:
  - SCADA and Telemetry
  - M2M (Machine to Machine)
  - Mobile
  - Web
  - IoT (Internet of Things)
MQTT: Key Features

Open
- An open published spec designed for the world of “devices”
  - Foundation technology for the Eclipse Foundation "Paho" M2M project

Simple
- Simple / minimal pub/sub messaging semantics
  - Simple set of verbs -- connect, publish, subscribe and disconnect.

Reliable
- Three qualities of service:
  - 0 – at most once delivery
  - 1 – assured delivery but may be duplicated
  - 2 – once and once only delivery
- In-built constructs to support loss of contact between client and server.
  - “Last will and testament” to publish a message if the client goes offline.
- Stateful “roll-forward” semantics and “durable” subscriptions.

Minimal
- Minimal on-the-wire format
  - Smallest possible packet size is 2 bytes
  - No application message headers
- Minimum communications/power
  - Push-based; no polling
  - Designed for minimal battery consumption
- Reduced complexity/footprint
  - Clients: C=30Kb; Java=100Kb
MQTT: Key Features

**Scalable**

- 240,000 concurrent clients tested with <5% CPU on a single IBM WebSphere MQ queue manager
  - We would have gone higher but the Lab ran out of load testing client machines

- By comparison:
  - Apache Web Servers max out at 25,000 connections

**Secure**

- Direct connection between your MQTT Broker and SCADA devices
- Network Encryption: TLS/SSL
- Authentication: JAAS
- Authorization: OAM; By Topic.
MQTT Lean Use of Bandwidth

### IBM Hursley Lab (UK) testing

<table>
<thead>
<tr>
<th>Scenario</th>
<th>HTTP</th>
<th>MQTT</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Get a single piece of data from the server</td>
<td>302 bytes</td>
<td>69 bytes</td>
</tr>
<tr>
<td></td>
<td>(~4 times)</td>
<td>(~4 times)</td>
</tr>
<tr>
<td>2. Put a single piece of data to the server</td>
<td>320 bytes</td>
<td>47 bytes</td>
</tr>
<tr>
<td></td>
<td>(~7 times)</td>
<td>(~7 times)</td>
</tr>
<tr>
<td>3. Get 100 pieces of data from the server</td>
<td>12600 bytes</td>
<td>2445 bytes</td>
</tr>
<tr>
<td></td>
<td>(~5 times)</td>
<td>(~5 times)</td>
</tr>
<tr>
<td>4. Put 100 pieces of data to the server</td>
<td>14100 bytes</td>
<td>2126 bytes</td>
</tr>
<tr>
<td></td>
<td>(~7 times)</td>
<td>(~7 times)</td>
</tr>
</tbody>
</table>

### European automobile manufacturer testing

**Vehicle Telematics**

Mobile Network Data Costs/Vehicle

<table>
<thead>
<tr>
<th>HTTPS</th>
<th>MQTT</th>
</tr>
</thead>
<tbody>
<tr>
<td>220€/vehicle</td>
<td>23€/vehicle</td>
</tr>
</tbody>
</table>
Built in Session Awareness

1. Connection to cell tower lost

2. MQTT-based Broker becomes aware of lost connection

3. MQTT-Broker becomes aware of lost connection; publishes Last Will and Testament

4. Session re-established via alternative link (e.g., Satellite)

Telco Command Center

Last Will & Testament
- Connection lost – reconnect via satellite

Cell Tower

MQTT Broker

Satellite

SCADA Device
IBM WebSphere Message Broker – the Universal Message Processor

- **Connectivity FROM anywhere, TO anywhere**
  - Simplifies application connectivity; Enables business flexibility

- **Simple Graphical Programming Environment with Pre-Built Patterns**
  - Graphical data flows represent application & service connectivity
    - Custom logic via Graphical mapping, PHP, Java, ESQL, XSL & WTX
  - Patterns for top-down, parameterized connectivity of common use cases

- **Comprehensive Protocols, Transports, Data Formats & Processing**
  - State of the art support for any kind of data formats -- XML, packed decimal, binary, SAP IDOC, etc.
  - Connects applications, services, systems and devices
  - Rich built-in suite of processor functions

- **Extensive Management, Performance & Scalability**
  - Extensive administration & systems management facilities
  - High performance transactional processing, additional vertical & horizontal scalability
  - Multiple deployment options include Trial, Express, Standard and Advanced

“Tools on Platforms” vs. “Coding on Operating Systems”

© 2012 IBM Corporation
Additional Components

- Mobile Dashboards
- Centralized Data Warehouse / Historian
- Centralized Event Correlation
- Enterprise Asset Management
Mobile SCADA Dashboards

Provide customized real-time device status to field technicians based on who they are and what they cover.
Centralized Historian – Combine and Replay Information

Maintain existing historian relationships...

...but combine information from multiple sources in a Centralized Warehouse / Historian for later replay and analysis.

Message Broker (w/Message Record and Replay)

SCADA Data

Other Data
Centralized Event Correlation – Get to Root Cause Faster

Correlation

Deduplication

SCADA Domain 1

SCADA Domain 2

SCADA Domain 3

Injection Site

Booster Station #1

Booster Station #2

Booster Station #N

Tank Farm

SCADA Domain 1 SCADA Domain 2 SCADA Domain 3
Enterprise Asset Management -- Reduce Mean Time to Resolution

Build information on the history and status of all your asset.

Consolidate point solutions for Asset AND Service Management.

Manage workflow anywhere in or beyond your enterprise.
Smarter SCADA – Summary

- Open Device Protocol (MQTT)
- Unified Intrusion Protection
- Tools on Platforms instead of Coding on Operating Systems
- Any-to-Any Connectivity
- Mobile Dashboards
- Enterprise Data Warehouse / Historian
- Centralized Event Correlation
- Enterprise Asset Management.
## Hands On Workshop

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
</tr>
</thead>
<tbody>
<tr>
<td>9:00am</td>
<td><strong>BREAK</strong></td>
</tr>
<tr>
<td>9:15am</td>
<td>Components of Smarter SCADA</td>
</tr>
<tr>
<td>9:30am</td>
<td>Smarter SCADA Connectivity</td>
</tr>
<tr>
<td>10:15am</td>
<td><strong>BREAK</strong></td>
</tr>
<tr>
<td>10:30am</td>
<td>Hands on Connectivity Workshop</td>
</tr>
<tr>
<td>12:30am</td>
<td><strong>LUNCH</strong></td>
</tr>
<tr>
<td>1:30pm</td>
<td>SCADA Device Security</td>
</tr>
<tr>
<td>1:45pm</td>
<td>Operational Control &amp; Decision Management</td>
</tr>
<tr>
<td>2:30pm</td>
<td><strong>BREAK</strong></td>
</tr>
<tr>
<td>2:45pm</td>
<td>Applying Smarter SCADA to your Scenarios</td>
</tr>
<tr>
<td></td>
<td>Next Steps</td>
</tr>
</tbody>
</table>